Telia

Relying Party Agreement
Release 2023-01-03

1. OVERVIEW

This is a Relying Party Agreement ("Agreement") between you ("Relying Party") and Telia Finland Oyj, a Helsinki based company ("Telia Certification Authority (CA)"). You must read this Agreement before assessing, using, or relying on any digital certificates or related certificate services or information provided by Telia CA. If you do not agree to the terms of this Agreement, do not submit a query to, and do not download, access, use, or rely on any aspect of, the Telia CA Public Key Infrastructure (PKI).

Telia Group Security Policy and Telia´s general delivery terms[1] apply to this document.

Certificates issued by Telia CA are utilized in connection with several security services offered by Telia or other parties. This Agreement includes the obligations and responsibilities for the users trusting, using or registration Telia certificates.

2. DEFINITIONS

Affiliate	A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.
Certification Authority (CA)	CA is an entity such as Telia that is authorized to create, sign, distribute, and revoke certificates. CA is also responsible for distributing certificate status information and providing a repository where certificates and certificate status information is stored.
CA/Browser Forum	A group of representatives from certificate authorities and browser vendors to discuss issues surrounding the existing market for server certificates, e.g., certificates used in authenticating TLS-enabled web sites and other servers (e.g., mail servers) to users.
Certificate	An electronic document issued by Telia to a person or entity mainly for verifying the identity of the sender/receiver of an electronic message, and/or for providing the means to encrypt/decrypt messages between sender and receiver (e.g., binding an entity to their public key).
Certificate Request	A process where a natural person (the Subscriber or someone employed by the Subscriber) or an authorized agent with the authority of representing the Subscriber that completes and submits a certificate requestion.
Client Certificate	A digital certificate in which information about the organization and email of holding the certificate has been validated by Telia.
Certificate Practice Statement (CPS)	CPS is a document that defines the legal, commercial and technical practices for approving, issuing, using and managing Telia Server and Client certificates. It also outlines the roles and responsibilities of the parties involved in maintaining the Telia public key infrastructure.
Digital Signature	A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.

[1] Delivery terms for business customers: https://www.telia.fi/dam/jcr:5f8ae50b-f587-4829-8499-c07028580d8b/Telias%20General%20Delivery%20Terms%20for%20Business%20Customers%20Concerning%20Services.pdf

Domain name	The label assigned to a node in the Domain Name System.
Domain Validated (DV) TLS Server Certificate	A digital certificate for a web site or other server in which the information about the domain name has been validated by Telia.
Registration Authority (RA)	An employee or agent of an organization unaffiliated with Telia who authorizes issuance of certificates to that organization.
Fully Qualified Domain Name (FQDN)	A domain name that specifies its exact location in the tree hierarchy of the Domain Name System.
OV TLS Server Certificate	A digital certificate in which information about the business entity holding the certificate has been validated by Telia.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Relying Party	Anybody who relies on the certificates issued by Telia (including all end users and operating system vendors who trust Telia certificates).
Repository	An online database containing publicly-disclosed Telia PKI governance documents, and certificate status information, either in the form of a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) response. https://cps.trust.telia.com.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Service Element	The CA internal systems, processes or services such as certificate enrolment, PKI support, backup and system monitoring.
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subscriber	A person or entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement and Terms of Use.
Subscriber Agreement	An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the CABF requirements when the Applicant/Subscriber is an Affiliate of the Telia CA or is the CA.

3. SERVICES

3.1 Certificate Types. The following certificate types ("Services") are offered by Telia: (i) **Telia TLS DV certificate:** to authenticate servers and establishing secure Transport Layer Security (TLS) sessions with end clients. In this type the domain name the server domain name is validated by Telia, (ii) **Telia TLS OV certificate:** to authenticate servers and establishing secure TLS sessions with end clients. In this type domain name of the server, existence of the organisation and other attributes including name, type, status, and physical address is validated by Telia, (iii) **Telia client certificate**: for identifying individual users, securing email communications and document signing, or (iv) **Telia document signing (Seal) certificate:** for authenticating documents from Adobe PDF, Microsoft Office, OpenOffice, and LibreOffice.

3.2 Certificate Request. In order for Subscriber to obtain a Certificate, the Subscriber shall submit a certificate request in a form specified by Telia for each ordered Certificate ("Certificate Request"). Forms for a Certificate Request are available on Telia CA's website and may be completed electronically.

3.3 Validation. Upon Telia's acceptance of Subscriber's Certificate Request, Telia validate the information provided in accordance with the applicable CPS. If Telia validates the Subscriber successfully, Telia issues the Certificate(s) to Subscriber. Telia may reject a Certificate Request and refuse to issue any ordered Certificate in its sole discretion.

3.4 Revocation. Telia may revoke a Certificate if Telia believes or has reason to believe that:

a) Subscriber requests a certificate revocation;
b) Telia CA obtains evidence that the certificate was misused;
c) Telia CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement and Terms of Use;
d) Telia CA is made aware of any circumstance indicating that use of a FQDN or IP address in the certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
e) Telia CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
f) Telia CA is made aware of a material change in the information contained in the certificate;
g) Telia CA is made aware that the certificate was not issued in accordance with the Baseline Requirements or the applicable CPS;
h) Telia CA determines or is made aware that any of the information appearing in the certificate is inaccurate;
i) Telia CA's right to issue certificates under the Baseline Requirements expires or is revoked or terminated, unless Telia CA has made arrangements to continue maintaining the CRL/OCSP Repository;
j) Revocation is required by Telia CA' applicable CPS; or
k) Telia CA is made aware of a demonstrated or proven method that exposes the Subscriber's private key to compromise, methods have been developed that can easily calculate it based on the public key, or if there is clear evidence that the specific method used to generate the private key was flawed.

After revoking a Certificate, Telia may, in its sole discretion, reissue the Certificate to Subscriber.

4. RELYING PARTY OBLIGATIONS

Telia provides two approaches to verify certificate validity using RFC6960: online status checking protocol (OCSP) and RFC5280: certificate revocation lists (CRLs) that are available at Telia CA's repository.

To be able to reasonably rely on a certificate a relying party shall at least:

- Verify the authenticity and validity of the certificate using common PKI rules (checking the certification path validation and certificate contents according to chapter 6 in RFC 5280),
- Verify from a valid CRL or via OCSP that the certificate has not been revoked or suspended,
- Check the intended key usage and extended key usage of the certificate, and
- Use the certificate legally and with no unauthorized purposes.

Note. Certain services offered by Telia include verification of the authenticity and validity of the certificate by Telia on behalf of the Subscriber.

5. WARRANTIES

5.1 Mutual warranties. Each party warrants that it has full power and authority to enter into and perform its obligations under the Agreement which, when agreed, will constitute binding obligations on the warranting party.

5.2 Usage. Telia CA makes no representation concerning the quality of the Services and does not promise that the Services will be free from error or compromise. Usage of the Telia CA Services is solely at the Relying Party's own risks.

6. LIABILITIES AND INDEMNITIES

6.1 Liabilities. Telia CA accepts no liability for damages incurred by the Relying Party accepting one of its certificates, or by a Subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by the Relying Party. It also accepts no liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with the applicable CPS.

6.2 Indemnities. Telia CA will not pay indemnities for damages arising from the use or rejection of certificates it issues.

7. TERMS AND TERMINATION

7.1 Term. Unless otherwise terminated as allowed herein, this Agreement is effective upon Relying Party's acceptance and lasts for as long as a Certificate issued under this Agreement is valid.

7.2 Termination. The term of this Agreement begins when the Relying Party has accepted its terms as provided in the preamble above. Either party may terminate this Agreement at any time, for any reason or no reason. Telia may provide notice through its Repository. On termination of this Agreement for any reason, the Relying Party will immediately cease use of Telia CA services.

8. PRIVACY CONSIDERATIONS

Telia does not collect any sensitive or confidential data from Relying Parties. The collected information will not be used for any other purpose and Telia's privacy policy[2] governs the CA operations. Telia's Privacy Notice applies to all processing of personal data[3].

9. DISPUTES

9.1 Good faith negotiations. Before taking any Court action, parties must use best efforts to resolve any dispute under through good faith negotiations.

9.2 Legal actions. Any disputes arising from or relating to this Agreement shall be finally settled by arbitration in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The number of arbitrators shall be one, unless the other party requires that the arbitral tribunal be composed of three members. The place of arbitration is Helsinki, Finland, and the language of the arbitration is Finnish. Without prejudice to the above, the parties have the right to bring a legal action at the Helsinki District Court when the value of the dispute does not exceed one hundred thousand (100,000) Euros.

9.3. Obligations continue. Each party must, to the extent possible, continue to perform its obligations under the Agreement even if there is a dispute.

9.4 Right to seek relief. This clause does not affect either party's right to seek urgent interlocutory and/or injunctive relief.

10. MISCELLANEOUS

10.1 Amendments. Relying Party will not be notified if the applicable CPS document is changed. When changes are made they will be published in the Repository for public review and after 15 days will be in effect. Changes to the Telia Group Security Policy will be communicated to third parties, where applicable.

10.2 Law. The Agreement is governed by, and must be interpreted in accordance with, the laws of Finland without regard to the conflict of law provisions.

11. CONSENT

By submitting any query to, or otherwise by downloading, accessing, using, or relying on any aspect of, Telia CA, you have accepted all terms of this Agreement and you are entitled to use the Telia CA Services included in this Agreement.

[2] Telia Group Policy - Privacy and Data Protection: https://www.teliacompany.com/globalassets/telia-company/documents/about-telia-company/public-policy/group-policy---privacy-and-data-protection.pdf

[3] https://www.telia.fi/tietosuoja-ja-tietoturva/privacy-notice